No. 16-1371

IN THE

Supreme Court of the United States

TERRENCE BYRD,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

On Writ of Certiorari to the
United States Court of Appeals for the Third Circuit

BRIEF OF *AMICI CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) AND TWENTY-THREE TECHNICAL EXPERTS AND LEGAL SCHOLARS IN SUPPORT OF PETITIONER

MARC ROTENBERG
Counsel of Record
ALAN BUTLER
ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
rotenberg@epic.org

November 20, 2017

TABLE OF CONTENTS

TABLE OF AUTHORITIES ii

INTEREST OF THE *AMICI CURIAE* 1

ARGUMENT 6

I. Modern cars collect and store vast troves of personal data. 7

A. A search of a modern vehicle can reveal extensive personal data. 8

II. Relying on rental contracts to negate Fourth Amendment standing would undermine legitimate expectations of privacy. 18

A. The status of the driver is irrelevant to Fourth Amendment privacy interests. 19

B. Constitutional rights are still recognized despite contractual violations. 24

CONCLUSION 25

TABLE OF AUTHORITIES

CASES

Katz v. United States,
389 U.S. 347 (1967) 20

Rakas v. Illinois,
439 U.S. 128 (1978) 24

Riley v. California,
573 U.S. __ (2014) 7

United States v. Jones,
565 U.S. 400 (2012) 18, 20, 21, 22, 23

United States v. Owens,
782 F.2d 146 (10th Cir. 1986) 24

United States v. Powell,
732 F.3d 361 (5th Cir. 2013) 24

STATUTES

18 U.S.C. § 2721 ..... 16, 17

OTHER AUTHORITIES

Allen & Overy, *Autonomous and Connected Vehicles: Navigating the Legal Issues* (2017) 8, 13

Andrew Meola, *Automotive Industry Trends: IoT Connected Smart Cars & Vehicles*, Bus. Insider (Dec. 20, 2016) 8

Automatic Emergency Breaking, My Car Does What 15, 16

Avis, *Privacy Notice* (2017) 11

Damon Lavrinc, *Progressive Insurance's Driver Tracking Tool lis Ridiculously Insecure*, Jalopnik (Jan. 20, 2015) 14

David Burnham, *The Rise of The Computer State* (1980) 25

Drowsiness Alert, My Car Does What 15

Edward H. Baker et al., *Connected Car Report 2016: Opportunities, Risk, and Turmoil on the Road to Autonomous Vehicles* (Sept. 28, 2016) 9

Enterprise, *Global Privacy Policy* (2017) 11, 13

EPIC, *Automobile Event Data Recorders (Black Boxes) and Privacy* 16

EPIC, *State Auto Black Boxes Policy* 17

High Speed Alert, My Car Does What 15

Jennifer Abel, Consumer Affairs, *Hertz Putting Passenger-compartment Cameras in Rental Cars* (Mar. 18, 2015) 10, 12

Jennifer Abel, Consumer Affairs, *Rental-car Drivers: Take These Important Steps to Protect Our Privacy* (July 13, 2015) 12

Joe Donovan, *Want to Know If your Phone Pairs with Your Car? This Handy List Should Do the Trick*, Digital Trends (Aug. 5, 2014) 12

Kelsey Mays, *Do Apple CarPlay, Android Auto Keep Data From Your Smarthphone?* Cars.com (March 28, 2016) 12, 13

Kim Komando, *Your Car's Hidden 'Black Box' and How to Keep It Private*, USA Today (Dec. 26, 2014) 16

Lisa Weintraub Schifferle, Fed. Trade Comm'n, *What Is Your Phone Telling Your Rental Car?* (Aug. 30, 2016) 7, 11, 12, 18

Marc Rotenberg, *Are Vehicle Black Boxes A Good Idea?*, Costco Connection (April 2013) 16

Marc Rotenberg, *Steer Clear of Cars that Spy*, USA Today (Aug. 18, 2011) 7, 16

Nat'l Conference of State Legislatures, *Privacy of Data from Event Data Records: State Statutes* (Jan. 4, 2016)..... 17

Nat'l Highway Traffic Safety Admin., *Event Data Recorder* 16

OnStar, *Driving Information and Data Collection* .. 14

OnStar, *Home*..... 13

OnStar, *Privacy Statement*..... 14

Press Release, Avis Budget Group, *Avis Car Rental Expands Fleet of Connected Cars* (May 22, 2017). 10

Progressive, *Frequently Asked Questions about Snapshot* *15*

Sen. Edward J. Markey (D-Mass), *Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk* (2015) 8, 9

U.S. Gov. Accountability Office, GAO-14-649T, *Consumers' Location Data: Companies Take Steps to Protect Privacy, but Practices Are Inconsistent, and Risks May Not be Clear to Consumers* (2014) 9, 10

World Economic Forum, *Digital Transformation of Industries Automotive Industry* (2016) 7

INTEREST OF THE *AMICI CURIAE*

The Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, D.C.[1] EPIC was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other constitutional values.

EPIC routinely participates as *amicus curiae* before this Court and other courts in cases concerning privacy issues, new technologies, and constitutional interests. *See, e.g.*, *Carpenter v. United States*, No. 16-402 (2017) (arguing that the Fourth Amendment protects the right against warrantless seizure and search of location data); *State v. Earls*, 214 N.J. 564 (2013) (same); *Packingham v. North Carolina*, 137 S. Ct. 1730 (2017) (arguing that the First Amendment protects the right to access speech from the privacy of a personal electronic device); *Utah v. Streiff*, 136 S. Ct. 2056 (2016) (arguing that evidence obtained via suspicionless identification should be suppressed); *Riley v. California*, 134 S. Ct. 2473 (2014) (arguing that it is unreasonable to warrantlessly search a cell phone incident to an arrest); *Florida v. Harris*, 133 S. Ct. 1050 (2013) (arguing that the government bears the burden of establishing the reliability of new investigative techniques used in establishing probable cause for a search); *United States v. Jones*, 565 U.S. 400 (2012) (arguing that warrantless tracking of a car using a

---

[1] Both parties consent to the filing of this brief. In accordance with Rule 37.6, the undersigned states that no monetary contributions were made for the preparation or submission of this brief, and this brief was not authored, in whole or in part, by counsel for a party.

GPS device violates the Fourth Amendment); *Commonwealth v. Connolly*, 454 Mass. 808 (2009) (same).

EPIC has also filed extensive comments with federal agencies and testified before the U.S. Congress regarding the privacy and consumer safety risks posed by connected vehicles. *See, e.g.*, Comments of EPIC to the National Highway Traffic Safety Administration/Department of Transportation (Nov. 14, 2017);[2] Comments of EPIC to the Federal Trade Commission & National Highway Traffic Safety Administration, EPIC (May 1, 2017);[3] *Self-Driving Vehicle Legislation: Hearing on H.R. 3388 Before the H. Comm. on Energy & Commerce*, 115th Cong. (2017) (statement of Marc Rotenberg, EPIC President);[4] Comments of EPIC to the National Highway Traffic Safety Administration Department of Transportation, EPIC (Nov. 22, 2016);[5] *The Internet of Cars: Joint Hearing Before the Subcomm. on Transp. & Pub. Assets of the H. Comm. on Oversight & Gov't Reform*, 114th Cong. (2015) (statement of Khaliah Barnes, Associate Director and Administrative Law Counsel, EPIC).[6] EPIC has repeatedly emphasized that there are unique privacy risks arising from modern vehicles that are not addressed in current law. *See* Marc Rotenberg, *Steer Clear of*

---

[2] https://epic.org/apa/comments/EPIC-NHTSA-AutomatedDrivingSystems.pdf.

[3] https://epic.org/apa/comments/EPIC-ConnectedCar-Workshop-Comments.pdf.

[4] https://epic.org/testimony/congress/EPIC-HEC-AV-Legislation-Jun2017.pdf.

[5] https://epic.org/apa/comments/EPIC-NHTSA-AV-Policy-comments-11-22-2016.pdf.

[6] https://epic.org/privacy/edrs/EPIC-Connected-Cars-Testimony-Nov-18-2015.pdf.

Cars that Spy, USA Today (Aug. 18, 2011);[7] Marc Rotenberg, *Are Vehicle Black Boxes A Good Idea?*, Costco Connection (April 2013).[8]

EPIC seeks to ensure that Fourth Amendment protections apply to policing practices that implicate new technologies. This case presents a fundamental question about the scope of Fourth Amendment protections as applied to the search of rental vehicles at a time when motor vehicles are being routinely equipped with devices that capture and record personal data. EPIC submits the following *amicus* brief, signed by distinguished technical experts and legal scholars, in support of the Fourth Amendment in the digital age.

Technical Experts and Legal Scholars

Rod Beckstrom
Founder and CEO, BECKSTROM

Colin J. Bennett
Professor, University of Victoria

Cynthia Dwork
Gordon McKay Professor of Computer Science, Harvard Radcliffe Alumnae Professor, Radcliffe Institute for Advanced Study

David J. Farber
Distinguished Career Professor of Computer Science and Public Policy, Carnegie Mellon University

---

[7] https://usatoday30.usatoday.com/news/opinion/editorials/2011-08-18-car-insurance-monitors-driving-snapshot_n.htm.

[8] http://www.costcoconnection.com/connection/201304?pg=24#pg24.

Addison Fischer
Founder and Chairman, Fischer International Corp.

Hon. David Flaherty
Former Information and Privacy Commissioner for British Columbia

Chris Larsen
Executive Chairman, Ripple, Inc.

Harry R. Lewis
Gordon McKay Professor of Computer Science, Harvard University

Anna Lysyanskaya
Professor of Computer Science, Brown University

Gary T. Marx
Professor Emeritus of Sociology, MIT

Mary Minow
2017-18 Fellow, Berkman Klein Center for Internet and Society at Harvard University

Eben Moglen
Professor of Law, Columbia Law School
Founding Director, Software Freedom Law Center

Dr. Pablo Garcia Molina
Adjunct Professor, Georgetown University

Dr. Peter G. Neumann
Senior Principal Scientist, SRI International Computer Science Lab

Dr. Deborah C. Peel, M.D.
Founder and Chair, Patient Privacy Rights

Ronald L. Rivest
Institute Professor of Electrical Engineering and Computer Science, MIT

Bruce Schneier
Program Fellow and Lecturer, Harvard Kennedy School

Robert Ellis Smith
Publisher, Privacy Journal

Nadine Strossen
John Marshall Harlan II Professor of Law, New York School; Former President, American Civil Liberties Union

Jim Waldo
Gordon McKay Professor of the Practice of Computer Science, Chief Technology Officer, John A. Paulson School of Engineering and Applied Science, Professor of Technology Policy, Harvard Kennedy School

Anne L. Washington, PhD
Data & Society Research Institute Fellow
Assistant Professor, Schar School of Policy and Government, George Mason University

Christopher Wolf
Board Chair, Future Privacy Forum

Shoshana Zuboff
Charles Edward Wilson Professor of Business Administration, Emerita, Harvard Business School

(Affiliations are for identification only)

SUMMARY OF THE ARGUMENT

The modern vehicle is not your dad's Chevy. The connected car is a computer on wheels. It stores vast troves of personal data, including the date, time, and location of the vehicle, as well as acceleration and braking patterns, weather conditions, and the identities of the occupants. An individual's entire address book can be quickly collected from a Bluetooth-connected device and stored within the vehicle. The car makes little distinction between driver and occupant, those on a rental agreement and those who are not. All of the personal data collected by the vehicle is stored, recorded, and available for later inspection.

In response to these new technologies, many states have established privacy safeguards for modern vehicles. Most have limited police access to the event data recorders, also known as "black boxes." These states are seeking to provide a ride safe from mass surveillance. But the bump in the road remains the absence of a clear Fourth Amendment rule to limit police access to personal data stored in the vehicle. That issue may not be obvious in this case. But if you look under the hood, you will see that the warrantless search of a modern vehicle implicates far more privacy interests than the physical search of a '66 Buick LeSabre.

EPIC also encourages the Court to steer clear of a Fourth Amendment ruling that relies on private contracts. That is a Fourth Amendment detour that leads to a dead end.

ARGUMENT

I. Modern cars collect and store vast troves of personal data.

A warrantless search of a vehicle today could expose much more than just the physical items around the seats. For example, a police officer could readily obtain the complete address book from an occupant's cell phone even though this Court has previously ruled that a similar search of a cell phone incident to arrest would require a warrant. *Riley v. California*, 573 U.S. __ (2014) (holding that the warrantless search of a cell phone seized subsequent to arrest is impermissible); *see also* Lisa Weintraub Schifferle, Fed. Trade Comm'n, *What Is Your Phone Telling Your Rental Car?* (Aug. 30, 2016).[9] It should make no difference whether the search of a vehicle was for a person named on a rental car agreement or not. Modern vehicles spy on both drivers and passengers. Marc Rotenberg, *Steer Clear of Cars that Spy*, USA Today (Aug. 18, 2011).

The automobile is undergoing a transformation. Modern vehicles contain "infotainment" systems that record location data and GPS trips visited while traveling in the rental car, along with a wide range of other personal data. By 2020, approximately 381 million connected vehicles will be on the road, and 90% of cars sold will have the capacity to connect to the Internet. World Economic Forum, *Digital Transformation of Industries Automotive Industry* 9 (2016);[10] Andrew Meola, *Automotive Industry Trends: IoT Connected Smart*

---

[9] https://www.consumer.ftc.gov/blog/2016/08/what-your-phone-telling-your-rental-car.

[10] https://www.accenture.com/t20170116T084448__w__/us-en/_acnmedia/Accenture/Conversion-Assets/WEF/PDF/Accenture-Automotive-Industry.pdf.

Cars & Vehicles, Bus. Insider (Dec. 20, 2016).[11] Connected vehicles, which store detailed personal data, will become the predominant form of private transportation in the near future.

A. A search of a modern vehicle can reveal extensive personal data.

Modern cars are computers on wheels. Today's vehicles contain dozens of small computers that are linked together by the car's internal computer network. *See* Allen & Overy, *Autonomous and Connected Vehicles: Navigating the Legal Issues* (2017);[12] Sen. Edward J. Markey (D-Mass), *Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk*, (2015) [hereinafter "Markey Report"].[13] These computers control everything from braking, acceleration, steering, engine performance, door locks, and climate control to navigation and entertainment. Allen & Overy, *supra*, at 2. Pre-installed technological systems collect a diverse set of data, including location data recorded at regular intervals; previous destinations entered into the navigation system; and last location parked. Markey Report, *supra*, at 8. These systems also collect operational data, such as vehicle speed; direction/heading of travel; distances and time traveled; average fuel economy/consumption; status of power windows, doors, and locks; tire pressures; fuel level; tachometer reading (engine RPM gauge); odometer

---

[11] http://www.businessinsider.com/connected-car-statistics-manufacturers-2015-2.

[12] http://www.allenovery.com/SiteCollectionDocuments/Autonomous-and-connected-vehicles.pdf.

[13] https://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf.

reading; mileage since last oil change; battery health; coolant temperature; engine status; exterior temperature and pressure. *Id.* Modern vehicles also connect "to the Internet and [contain] a variety of sensors, and . . . are thus able to send and receive signals, sense the physical environment around them, and interact with other vehicles or entities." Edward H. Baker et al., *Connected Car Report 2016: Opportunities, Risk, and Turmoil on the Road to Autonomous Vehicles* 10 (Sept. 28, 2016).[14]

Soon, connected vehicles will collect data about "driving patterns, touch point preferences, digital service usage, and vehicle condition." *Id.* at 21. As cars become increasingly connected, they will collect and store more and more sensitive data about the driver and other occupants of the vehicle. According to a 2015 Senate report, about a third of all cars from 13 major car manufacturers collect data about driving history. Markey Report, *supra*, at 8. This includes "navigation, telematics, infotainment, emergency assist, stolen vehicle recovery, and event data recording systems." *Id.* This data would reveal where a car was driven and how the car was driven, and could also include the identity of drivers or occupants. *Id.* Telematics systems "use telecommunication networks and GPS signals to allow information, such as location data, to be communicated between a car and a service provider." U.S. Gov. Accountability Office, GAO-14-649T, *Consumers' Location Data: Companies Take Steps to Protect Privacy, but Practices Are Inconsistent, and Risks May Not be Clear to Consumers* (2014).[15]

---

[14] http://www.strategyand.pwc.com/media/file/Connected-car-report-2016.pdf.

[15] http://gao.gov/products/GAO-14-649T.

According to a GAO study, the collection and disclosure of consumer location information by in-car navigation providers poses serious risks to consumer privacy. *Id.* at 2. Storing location information over time "create[s] a detailed profile of individual behavior, including habits, preferences, and routes traveled," the exploitation of which can lead to identity theft or threats to personal safety. *Id.*

Rental cars are increasingly equipped with systems that collect personal data about drivers and occupants. Presently, "1 out of 8 cars in Hertz's rental fleet are equipped with dashboard cameras – not outward-facing cameras monitoring the road, but inward-facing cameras capable of making audio and video recordings of everything inside the passenger compartment." Jennifer Abel, Consumer Affairs, *Hertz Putting Passenger-compartment Cameras in Rental Cars* (Mar. 18, 2015).[16] Avis recently announced that it would double the number of connected vehicles in its fleet by 2018, raising the overall number to 100,000. Press Release, Avis Budget Group, *Avis Car Rental Expands Fleet of Connected Cars* (May 22, 2017).[17] Avis specifies that its vehicles are "equipped with devices which allow [Avis] to send commands to and receive certain information from the vehicle, including geolocation data from a global positioning system (GPS). These devices are turned on all the time, even when other services or other media in the vehicle is turned off." Avis,

---

[16] https://www.consumeraffairs.com/news/hertz-putting-passenger-compartment-cameras-in-rental-cars-031815.html

[17] *Available at* http://ir.avisbudgetgroup.com/releases.cfm?Year=&ReleasesType=&PageNum=2.

Privacy Notice 3 (2017).[18] Avis further specifies that the devices "collect and process vehicle data about the vehicle itself, such as fuel level, odometer, speed, diagnostic and performance data, tire pressure, accident or damage data, and location and direction of travel data." *Id.* Enterprise rental vehicles also contain telematics systems, which collect (1) location information, (2) crash notification and related crash data, and (3) operational condition, mileage, diagnostic and performance reporting of vehicles. Enterprise, *Global Privacy Policy* (2017).[19] The company claims that it is "not responsible for any data that is left in the vehicle" and that it "cannot guarantee the privacy or confidentiality of such information." *Id.* Rental car companies even "collect photos and videos in some instances, such as when you link your [Avis] account with your social media profile." *See, e.g.*, Avis, *Privacy Notice* 3 (2017).

Rental vehicles also contain "infotainment" systems that collect personal data stored on a driver's cell phone. Schifferle, *supra*. These systems are designed to "pair" an occupant's phone with the vehicle's audio and media system. But once a phone is connected, the car automatically downloads a vast amount of information from the driver's cell phone, including private contacts and messages. *Id.*

The amount of personal data a modern vehicle can collect varies by Bluetooth module "but typically there is storage for hundreds if not thousands of phone numbers." Kelsey Mays, *Do Apple CarPlay, Android Auto Keep Data From Your Smarthphone?* Cars.com

---

[18] https://www.avis.com/content/dam/avis/na/us/common/pdf-files/4433_AV_COM_terms_update_01.30.17.pdf.

[19] https://www.enterprise.com/en/privacy-policy.html.

(March 28, 2016).[20] According to technology analyst at HIS Automotive, Colin Bird, advanced Bluetooth systems collect and store data "including keystroke data, wireless sensor reporting and the ability to transmit short data packets like messages, emails, calendar notifications, tasks, notes and reminders." *Id.* Some cars even collect data from the occupants' social media accounts such as Facebook and Twitter. Joe Donovan, *Want to Know If your Phone Pairs with Your Car? This Handy List Should Do the Trick*, Digital Trends (Aug. 5, 2014) (providing a detailed list of automakers and their Bluetooth capabilities).[21] The car also collects call logs and any contacts from the phone. *Id.* This personal data is stored in the vehicle. Schifferle, *supra; see also* Jennifer Abel, Consumer Affairs, *Rental-car Drivers: Take These Important Steps to Protect Our Privacy* (July 13, 2015).[22] Stefan Cross, communications manager for GM's connected-car division warned that someone could easily access the Bluetooth module and get an occupant's phonebook, recent messages and other basic information, such as the name of the phone and Bluetooth key. Mays, *supra*. Furthermore, even if an occupant deletes his phone from the vehicle, only the "pointer" or "map" that shows where the data stored in the system is erased. *Id.* The actual content of the data is embedded memory and remains in the

---

[20] https://www.cars.com/articles/do-apple-carplay-android-auto-keep-data-from-your-smartphone-1420684038897/.

[21] https://www.digitaltrends.com/cars/automobile-bluetooth-compatibility/.

[22] https://www.consumeraffairs.com/news/rental-car-drivers-take-these-important-steps-to-protect-your-privacy-071315.html.

system's database. *Id.* A warrantless search of a vehicle would provide access to this sensitive personal data.

Modern vehicles incorporate social media apps, too. For example, "BMW's ConnectedDrive system has Facebook, Twitter and a Wiki Local app (which acts like an in-car travel guide), Mercedes-Benz's 'mbrace' system uses Yelp to help find restaurants and Audi Connect lets drivers not only find parking at their destination, but also reserve and pay for a space." Allen & Overy, *supra*, at 18 (internal citations added). Furthermore, "[t]he Audi Picture Navigation app allows users to use the location metadata embedded in a photo sent from a contact to plot a destination on the car's navigation system." *Id.* Soon to come, the University of Michigan has partnered with Ford, Microsoft and Intel to develop the Caravan Tracker app that enables multiple cars on a trip to connect and share information about how much petrol is left in the fuel tanks, to compare fuel economy, and to share route information. *Id.* All of these apps and personal data collected therefrom are and will become accessible within the vehicle.

Some rental vehicles collect driver and occupant data through the OnStar system, which is owned by General Motors and provides certain navigation and emergency access functions. *See, e.g.*, Avis, *Privacy Notice* 3 (2017); Enterprise, *Global Privacy Policy* (Oct. 9, 2017). OnStar collects a broad range of data to facilitate communications with drivers and occupants, in-vehicle security, hands-free calling, turn-by-turn navigation, and remote diagnostics systems. OnStar, *Home*.[23] This data includes "specific driving behavior,

---

[23] https://www.onstar.com/us/en/home.html.

including hard braking events, hard acceleration events, time spent idle, speeds over 80 miles per hour, when a trip occurs and the number of miles driven." OnStar, *Driving Information and Data Collection*.[24] According to OnStar's Privacy Policy, OnStar collects "GPS location, speed, air bad deployments, crash avoidance alerts, impact data, safety system status, braking and swerving/concerning events, event data recorder (EDR) data, seatbelt settings, vehicle direction (heading), camera image and sensor data, voice command information, stability control or anti-lock events, security/theft alerts, infotainment system usage, and WiFi data usage." OnStar, *Privacy Statement*.[25] OnStar acknowledges that this data collection will occur with whomever operates an OnStar equipped vehicle; for example, "you let someone else drive your OnStar equipped vehicle." *Id.* In this case, OnStar's Privacy Statement still applies. *Id.*

Insurance companies have also introduced new techniques that collect data about a driver that could be subject to a law enforcement search. For example, Progressive's Snapshot device plugs into cars' OBDII ports to track a user's driving habits with the incentive that the user will lower his insurance rate. Damon Lavrinc, *Progressive Insurance's Driver Tracking Tool lis Ridiculously Insecure*, Jalopnik (Jan. 20, 2015).[26] Currently, the device has over two million users. *Id.* The Snapshot device logs location data and "collects

---

[24] https://www.onstar.com/us/en/help-support/onstar-smart-driver/driving-info-data-collection.html.

[25] https://www.onstar.com/us/en/footer-links/privacy-policy.html.

[26] https://jalopnik.com/progressive-insurances-driver-tracking-tool-is-ridicul-1680720690.

information about how you drive, how much you drive and when you drive. It also collects your vehicle identification number and triggers an email to you if it comes unplugged. Some devices collect location data." Progressive, *Frequently Asked Questions About Snapshot*.[27] Snapshot even collects phone usage data, including phone calls, texting, apps, and so forth. *Id.*

Connected vehicles even collect information about the driver without their knowledge by aggregating and analyzing data. This data could also be obtained in a law enforcement search. For example, some cars have a "drowsiness alert" that triggers based on certain driving data. *Drowsiness Alert*, My Car Does What.[28] The alert detects "drowsy" driving by tracking driving habits, such as lane departure. "High speed alert" gathers information about a vehicle's position, via GPS, with a database of speed limit information to warn a driver if they are speeding. *High Speed Alert*, My Car Does What.[29] Some vehicles even have a camera that can read speed limit signs to determine whether the driver is speeding. *Id.* "Automatic emergency breaking" systems scan the road in front of the vehicle and warn the driver of an impending crash, but can also collect data about whether the driver does not react in time. *Automatic Emergency Breaking*, My Car Does What.[30] The braking technique relies on either

---

[27] https://www.progressive.com/auto/discounts/snapshot/snapshot-common-questions/.

[28] https://mycardoeswhat.org/safety-features/drowsiness-alert/.

[29] https://mycardoeswhat.org/safety-features/high-speed-alert/.

[30] https://mycardoeswhat.org/safety-features/automatic-braking/.

camera- or radar-based sensors located in the front of the vehicle to detect proximity between vehicles. *Id.*

Today's vehicles also include built-in event data recorders, otherwise known as "black boxes." *See generally*, EPIC, *Automobile Event Data Recorders (Black Boxes) and Privacy*.[31] Black boxes record the events and actions of the driver, including speed, braking, turning, and use of a safety belt before a collision. Nat'l Highway Traffic Safety Admin., *Event Data Recorder*.[32] Black boxes "may record (1) pre-crash vehicle dynamics and system status, (2) driver inputs, (3) vehicle crash signature, (4) restraint usage/deployment status, and (5) post-crash data such as the activation of an automatic collision notification (CAN) system." *Id.*; *see also* Kim Komando, *Your Car's Hidden 'Black Box' and How to Keep It Private*, USA Today (Dec. 26, 2014).[33] Law enforcement and insurers could seek to use this information to make "determinations about liability and rates based on the data gathered by EDRs." Marc Rotenberg, *Are Vehicle Black Boxes A Good Idea?*, Costco Connection (April 2013); *see also* Marc Rotenberg, *Steer Clear of Cars That Spy*, USA Today (Aug. 18, 2011). In 2013, approximately 96% of all new cars sold in the U.S. contained a black box, and by September 1, 2014, every new vehicle required one. *Id.*

In response to growing privacy concerns related to black boxes, the federal government enacted the Driver Privacy Act of 2015. 18 U.S.C. § 2721, Pub. L.

---

[31] https://epic.org/privacy/edrs/.

[32] https://www.nhtsa.gov/research-data/event-data-recorder.

[33] https://www.usatoday.com/story/tech/columnist/komando/2014/12/26/keep-your-car-black-box-private/20609035/.

No. 114-94, 129 Stat. 1712 (2015); *see also* Nat'l Conference of State Legislatures, *Privacy of Data from Event Data Records: State Statutes* (Jan. 4, 2016).[34] The Act placed limits on access to black box data and guaranteed that the information collected belongs to the owner or lessee of the vehicle. 18 U.S.C. § 2721.

The states have also passed laws to give individuals control over the personal data gathered in modern vehicles. Seventeen states have enacted statutes governing black boxes and privacy: Arkansas, California, Colorado, Connecticut, Delaware, Maine, Montana, Nevada, New Hampshire, New Jersey, New York, North Dakota, Oregon, Texas, Utah, Virginia and Washington. Nat'l Conference of State Legislatures, *Supra*; *see* EPIC, *State Auto Black Boxes Policy*.[35] For example, in California, except for safety research or for auto diagnostics, one must obtain a court order and the owner's consent to download the data. *Id.* Arkansas, North Dakota and Oregon laws prohibit requiring owners to disclose their data as a condition of an insurance payment or settlement. *Id.* Furthermore, more than a dozen states require written notice to owners of the use of event data recorders. *Id.*

As newer technologies and recent legal developments make clear, modern vehicles raise many far-reaching privacy concerns that a Fourth Amendment analysis cannot ignore. Moreover, none of the techniques currently used in modern vehicles to collect personal data draw a distinction between those who are on a rental agreement and those who are not. The Third Circuit's bright-line distinction between these

---

[34] http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-of-data-from-event-data-recorders.aspx.

[35] https://epic.org/state-policy/edr/.

two categories of drivers is entirely disconnected from the scope of personal data that could be obtained from the vehicle.

Even the contractual relationship affords little protection. A rental agreement runs for a specific duration, but the data storage may extend well beyond that period. Once a rental vehicle has been returned to its dispatcher and the agreement has expired, the Third Circuit's holding establishes that the driver is no longer subject to the agreement; therefore, the driver would not have Fourth Amendment protection against the subsequent warrantless search of the data stored in the vehicles. Subsequent rentals users, employees, hackers, and even law enforcement officials could access information collected and stored through connecting personal devices in the vehicle. Schifferle, *supra*. Consequently, the Third Circuit's bright-line rule would significantly expand the scope of warrantless searches of driver data.

II. Relying on rental contracts to negate Fourth Amendment standing would undermine legitimate expectations of privacy.

This Court has held that the Fourth Amendment limits the ability of the government to track the location of a vehicle without regard to whether the driver is the owner of the vehicle or named on a rental car agreement. *United States v.* Jones, 565 U.S. 400 (2012). In *Jones*, the Fourth Amendment analysis did not turn on the status of the driver but on the conduct of the police. In three different opinions, the Court found that the warrantless tracking of the vehicle by

means of new technology violated the Fourth Amendment. Whether the driver was the owner or the renter was irrelevant.

A. The status of the driver is irrelevant to Fourth Amendment privacy interests.

This Court made clear in *United States v. Jones* that significant privacy interests are implicated by the tracking and collection of data from automobiles. While the Court disagreed over whether a property-based interest or the reasonable expectation of privacy analysis was the best route to take, the Justices ended up at the same destination and unanimously agreed that the warrantless search of a vehicle equipped with tracking technology violated the Fourth Amendment.

Justice Scalia emphasized in his opinion for the Court that where police conduct violates property-based interests, it triggers the Fourth Amendment:

> [T]he Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a "search." It is important to be clear about what occurred in this case: The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a "search" within the meaning of the Fourth Amendment when it was adopted . . . . The text of the Fourth Amendment reflects its close connection to property, since otherwise it would have referred simply to "the right of the people to be secure against unreasonable searches and

> seizures"; the phrase "in their persons, houses, papers, and effects" would have been superfluous . . . . Jones, who possessed the Jeep at the time the Government trespassorily inserted the information-gathering device, is on much different footing . . . . By attaching the device to the Jeep, officers encroached on a protected area.

Jones, 565 U.S. at 404, 405, 410. Justice Scalia's opinion did not turn on the status of the driver, even though the vehicle was not registered to the defendant. Instead, Justice Scalia emphasized that the "government physically occupied private property for the purpose of obtaining information." *Id.* at 404. The occupation of this private property constituted a search under the Fourth Amendment, regardless of to whom the vehicle belonged. *Id.* at 405. Therefore, under the property-based view, the status of the driver did not dictate the scope of Fourth Amendment protection.

In his concurring opinion in *Jones*, joined by four others, Justice Alito reasoned that the police tracking of the vehicle triggers the Fourth Amendment under the reasonable expectation of privacy test, established in *Katz v. United States*, 389 U.S. 347, 351 (1967):

> [T]he use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses, society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of

> an individual's car for a very long period. In this case, for four weeks, law enforcement agents tracked every movement that respondent made in the vehicle he was driving. We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark.

Jones, 565 U.S. 430. Justice Alito's analysis also did not depend on the status of the driver. Instead, Justice Alito focused on the *use* of the GPS for long-term tracking. *Id.* at 424. Long-term monitoring can occur even when the government has not committed a technical trespass (e.g. manufacturers including a GPS tracking device in every car). *Id.* A driver still maintains a reasonable expectation of privacy in the data collected from long-term tracking, regardless of if this data is retrieved through a GPS device already installed in the vehicle or placed by the government. *Id.* Despite a lack of ownership of the vehicle, Justice Alito found that a defendant had a reasonable expectation of privacy in the long-term monitoring of his driving habits. Most importantly, the status of the driver was not determinative in Justice Alito's reasonable expectation of privacy analysis.

In a separate concurring opinion in *Jones*, Justice Sotomayor set out a hybrid analysis that suggested that the case be resolved under both the property test and the reasonable expectation of privacy test:

> [A]s Justice Alito notes, physical intrusion is now unnecessary to many forms of surveillance. With increasing regularity,

> the Government will be capable of duplicating the monitoring undertaken in this case by enlisting factor- or owner-installed vehicle tracking devices or GPS-enabled smartphones. In cases of electronic or other novel modes of surveillance that do not depend upon a physical invasion on property, the majority opinion's trespassory test may provide little guidance. But "[s]ituations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis." *Ante*, at 953. As Justice Alito incisively observes, the same technological advances that have made possible nontrespassory surveillance techniques will also affect the *Katz* test by shaping the evolution of societal privacy expectations. *Post*, at 962-963. Under that rubric, I agree with Justice Alito that, at the very least "long term GPS monitoring in investigations of most offenses impinges on expectations of privacy."

Jones, 565 U.S. at 414–15 (internal citations omitted). Justice Sotomayor's analysis similarly did not turn on the status of the driver. She recognized that the Fourth Amendment is concerned not only with trespassory intrusions on property, but also when the government's conduct violates a subjective expectation of privacy. *Id.* Unlike Justice Alito, Justice Sotomayor found that even aspects of short-term surveillance could violate a reasonable expectation of privacy. *Id.* at 415. The analysis should focus on "whether people

reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on," not whether one can claim ownership over an object or space. *Id.* In fact, Justice Sotomayor pointed to precisely the problem presented in the search of the modern vehicle (the proliferation of data collection):

> It may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers.

Id. (emphasis added). Furthermore, Justice Sotomayor emphasized that she would "not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection." *Id.* In other words, the Court should steer clear of an analysis that relies on the status of the driver and follow the right sign marked "information involuntarily disclosed to others" to ascertain whether there is a reasonable expectation of privacy in the modern vehicle.

As the various opinions in *Jones* make clear, regardless of the Fourth Amendment road followed, the status of the driver, named on the rental agreement or not, is simply a detour and has no bearing on the Fourth Amendment outcome.

B. Constitutional rights are still recognized despite contractual violations.

The courts have recognized that the scope of the Fourth Amendment should not be dictated by "[s]ubtle distinctions" of state consumer protection laws or contracts. *United States v. Owens*, 782 F.2d 146, 150 (10th Cir. 1986) (citing *Jones v. United States*, 362 U.S. 257, 266 (1960) and *Katz v. United States*, 389 U.S. 347 (1967)). Courts should not rely on whether a person's name appears on a consumer contract to determine whether they have a constitutionally protected privacy interest as against the government. This is true not only of rental agreements, but also all commercial services governed by contracts, including, for example, the use of cell phones. *See, e.g., United States v. Powell*, 732 F.3d 361, 374 (5th Cir. 2013) (holding that a defendant disclaiming a personal connection to the phone discovered in the vehicle lacked a legitimate expectation of privacy in the phone being searched, regardless of who the phone actually belonged to). Furthermore, the Court has found that "arcane distinctions developed in property and tort law . . . ought not . . . control" the reasonableness of an expectation of privacy. *Rakas v. Illinois*, 439 U.S. 128, 143 (1978).

Yet the bright-line rule offered in this case would carry forward a distinction without constitutional significance and would fail to recognize the privacy interests of all driver and other occupants subject to a warrantless search.

* * *

The use of data generated by a rental vehicle is not a new privacy problem. David Burnham, *The Rise of The Computer State* 39–40 (1980) (describing police access to the "Wizard of Avis" to track the location of those who rent cars). But the routine collection of detailed personal data in modern vehicles is new and will become more acute in the years ahead.

Before the Court heads down the road of warrantless car searches in the modern vehicle, we write to warn that there is a caution sign ahead: "this will permit police access to the same data that the Court held in *Jones* would require a warrant." A better route is the one marked "Fourth Amendment warrant requirement."

CONCLUSION

For the foregoing reasons, *amici* respectfully ask this Court to reverse the decision of the U.S. Court of Appeals for the Third Circuit.

Respectfully submitted,

MARC ROTENBERG
ALAN BUTLER
ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
(202) 483-1248 (fax)
rotenberg@epic.org

November 20, 2017